**UNITED STATES DISTRICT COURT**
**FOR THE DISTRICT OF MASSACHUSETTS**

PRESTON LEONARD, individually and on behalf of all others similarly situated,

Plaintiff,

v.

ANNA JAQUES HOSPITAL, and BETH ISRAEL LAHEY HEALTH, INC.

Defendant(s).

Case No. _____

**CLASS ACTION COMPLAINT**

**DEMAND FOR JURY TRIAL**

Plaintiff Preston Leonard ("Plaintiff"), individually and on behalf of all others similarly situated (collectively, "Class members"), by and through his attorneys, brings this Class Action Complaint against Defendant Anna Jaques Hospital ("AJH") and Beth Israel Lahey Health, Inc. ("BILH") (collectively, "Defendant") and complains and alleges upon personal knowledge as to himself and information and belief as to all other matters.

## INTRODUCTION

1. Plaintiff brings this class action against AJH and BILH for their failure to secure and safeguard his and other similarly situated individuals' personally identifiable information ("PII") and personal health information ("PHI") (collectively "PII/PHI" or "Private Information"), that varies by individual. The breached information includes: names, date of birth, medical information, health insurance information, patient name, and patient address, demographic information, Social Security number, driver's license number, financial information, and other personal or health information that patients provided to AJH.

2. Defendant Anna Jaques Hospital is a multi-location hospital that offers services to the Merrimack Valley, North Shore, and Southern New Hampshire areas.

3. Defendant Beth Israel Lahey Health oversees a network of community hospitals, specialty hospitals, academic medical centers, and teaching hospitals, including Anna Jaques Hospital. The hospitals in the BILH system are located across Massachusetts and New Hampshire.

4. Upon information and belief, AJH is the only hospital system within the BILH network that was affected by this Data Breach. For the purposes of this Complaint, AJH, a part of BILH, will be referred to collectively as "Defendant."

5. On or about December 25, 2023, AJH identified suspicious activity on its network. Its investigation determined that AJH's network was subject to a data security event, resulting in the access, exposure and acquisition of files containing approximately 316,342 persons' (including Plaintiff's) personally identifying information ("PII") and personal health information ("PHI") (the "Data Breach").

6. On January 26, 2024, the Money Message ransomware group published the entirety of the PII/PHI stolen from Defendant on its dark web site.

7. On or about December 5, 2024, almost a full year after learning of the incident, AJH began sending notices to people whose PII and PHI (collectively "Private Information") was impacted by Data Breach. This notification delay is unreasonable and prevented Plaintiff and others from being able to mitigate their injuries promptly.

8. AJH, as well as its parent health system BILH, owed a duty to Plaintiff and Class members to implement and maintain reasonable and adequate security measures to secure, protect, and safeguard their PII/PHI against unauthorized access and disclosure. Defendant breached that duty by, among other things, failing to implement and maintain reasonable security procedures and practices to protect its patients' PII/PHI from unauthorized access and disclosure.

9. As a result of AJH and/or BILH's inadequate security and breach of its duties and obligations, the Data Breach occurred, and Plaintiff's and Class members' PII/PHI was accessed and disclosed. This action seeks to remedy these failings and their consequences. Plaintiff brings this action on behalf of himself and all natural persons whose Private Information was potentially compromised in the Network Incident, who were sent a notice by AJH that their PII/PHI was or may have been compromised in the Data Breach.

10. AJH failed to fulfill this obligation, as unauthorized cybercriminals breached AJH's information systems and databases and stole vast quantities of Private Information belonging to AJH's patients, including Plaintiff and Class members. The Data Breach—and the successful exfiltration of Private Information—were the direct, proximate, and foreseeable results of multiple failings on the part of AJH.

11. The Data Breach occurred because AJH failed to implement reasonable security protections to safeguard its information systems and databases. Moreover, before the Data Breach occurred, AJH failed to inform the public that its data security practices were deficient and inadequate. Had Plaintiff and Class members been made aware of this fact, they would have sought treatment elsewhere or would not have provided their Private Information to AJH.

12. As a result of AJH's negligent, reckless, intentional, and/or unconscionable failure to adequately secure its computer network, it failed to satisfy its contractual, statutory, and common-law obligations. As a result, Plaintiff and Class members suffered injuries, but not limited to: 1) lost or diminished value of their Private Information; 2) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information; 3) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to the loss of time to avoid or

resolve fraudulent charges; 4) time required to investigate, correct and resolve unauthorized access to their accounts; 5) time needed to deal with spam messages and e-mails received subsequent to the Data Breach; 6) loss of privacy; and 7) a substantial and imminent risk that their Private Information, which remains in Defendant's possession, will be subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect their Private Information.

13. Plaintiff, individually and on behalf of all other Class members, asserts claims for negligence, breach of fiduciary duty, breach of implied contract, and unjust enrichment, and seeks declaratory relief, injunctive relief, monetary damages, statutory damages, punitive damages, equitable relief, and all other relief authorized by law.

## PARTIES

14. **Plaintiff Preston Leonard** is a citizen and resident of South Hampton, New Hampshire. Plaintiff Leonard formerly received medical services from AJH. He provided his PII/PHI to AJH in connection with receiving healthcare services. He received a letter from AJH dated December 5, 2024, notifying him that his PII/PHI was involved in the Data Breach.

15. **Defendant Anna Jaques Hospital** is a Massachusetts nonprofit corporation with its principal place of business located at 25 Highland Ave., Newburyport, MA 01950.

16. **Defendant Beth Israel Lahey Health, Inc.** is a Massachusetts nonprofit corporation with its principal place of business located at 20 University Rd., Suite 700, Cambridge, MA 02138.

## JURISDICTION AND VENUE

17. This Court has subject matter jurisdiction over Plaintiff's claims under 28 U.S.C. § 1332(d)(2), because (a) there are 100 or more Class members, (b) at least one Class member is a

citizen of a state that is diverse from Defendants' citizenship, and (c) the matter in controversy exceeds $5,000,000, exclusive of interest and costs.

18. This Court has general personal jurisdiction over Anna Jaques Hospital and over Beth Israel Lahey Health, Inc., because they are both Massachusetts corporations and they each maintain their principal places of business in Massachusetts.

19. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because Defendants' principal places of business are in this District and a substantial part of the events, acts, and omissions giving rise to Plaintiff's claims occurred in this District.

## FACTUAL ALLEGATIONS

20. Defendant Anna Jaques is a "not-for-profit community hospital serving the Merrimack Valley, North Shore and Southern New Hampshire areas."[1]

21. As part of its normal business operations, AJH collects, maintains, and stores large volumes of Private Information belonging to its current and former patients.

22. In the regular course of its business, AJH collects and maintains the PII/PHI of patients, former patients, and other persons to whom it is currently providing or previously provided health-related or other services, and other affiliated persons.

23. AJH requires patients to provide personal information before it provides them services. That information includes, *inter alia*, names, Social Security numbers, driver's license information, payment information, dates of birth, medical record information, and health insurance information, among other data points. AJH stores this information digitally.

24. Current and former patients of AJH, such as Plaintiff and Class members, are required to provide a wealth of their own Private Information to AJH in exchange for medical

[1] About Anna Jaques Hospital, https://ajh.org/about (last accessed Dec. 23, 2024).

treatment and services. These patients, including Plaintiff and the Class, provided that Private Information with the reasonable expectation that AJH and any of its employees and agents who might have access to this information would keep it confidential and secure from illegal and unauthorized access. Plaintiff and the Class also expected that, in the event of any unauthorized access, AJH would provide them with prompt and accurate notice.

25. Defendant Beth Israel Lahey Health, Inc. ("BILH") is a healthcare system that includes "academic medical centers and teaching hospitals, specialty and community hospitals, more than 4,700 physicians and 39,000 employees."[2] Defendant AJH is a part of the BILH system.

26. Plaintiff's and Class member's expectations that AJH and BILH would protect their Private Information were objectively reasonable and based on an obligation imposed on AJH and BILH by statute, regulations, industrial custom, and standards of general due care, as well as its own promises of privacy made directly to its patients.[3]

27. However, Defendant(s) failed to carry out its duty to safeguard sensitive Private Information and provide adequate data security. As a result, it failed to protect Plaintiff and Class members' Private Information, which was accessed and stolen during the Data Breach.

28. In their virtually identical Notices of Privacy Practices ("Privacy Policy") provided to patients online and in-person, AJH and BILH acknowledge their legal obligations to protect the privacy of its patients. [4]

---

[2] https://bilh.org/about (last accessed Dec. 23, 2024).

[3] *See Notice of Privacy Practices*, BILH: https://bilh.org/-/media/files/bilh/bilh-privacy-practices-notice-2022.pdf; and *Notice of Privacy Practices*, AJH, https://ajh.org/-/media/files/bilh/bilh-privacy- practices-notice-2022.pdf (last accessed Dec. 23, 2024).

[4] *Id*.

*29.* Plaintiff and Class members are, or were, patients of AJH or received health-related or other services from AJH, and entrusted AJH with their Private Information.

***The Data Breach***

30. Per its breach notification letter, on or about December 25, 2024, AJH discovered unauthorized activity on its computer network. Its investigation showed cybercriminals had access to and did in fact breach AJH's information systems that contained confidential patient information. *See* Exhibit A.

31. On information and belief, AJH posted a notice on its website on January 24, 2024, but did not even begin to notify patients about the Data Breach until on or about December 5, 2024, **almost one year after it learned of the breach**.[5]

32. The Notice letter AJH posted on its website (*see* attached as Exhibit A, "Notice Letter") reveals that the information accessed by cybercriminals includes names, "demographic information, medical information, health insurance information, Social Security number, driver's license number, financial information, and other personal or health information that [patients] provided Anna Jaques."

***AJH Knew that Criminals Target PII/PHI***

33. At all relevant times, AJH knew, or should have known, its patients' PII/PHI was a target for malicious actors. Despite such knowledge, AJH failed to implement and maintain

[5] https://ajh.org/news-stories/all-news-stories/news/2024/01/information-about-anna-jaques-hospital-cybersecurity-incident

reasonable and appropriate data privacy and security measures to protect Plaintiff's and Class members' PII/PHI from cyber-attacks that AJH should have anticipated and guarded against.

34. Cybercriminals seek out PII/PHI at a greater rate than other sources of personal information. In a 2021 report, the healthcare compliance company Protenus found that there were 758 medical data breaches in 2020, with over 40 million patient records exposed.[6] This was an increase from the 572 medical data breaches that Protenus compiled in 2019.[7] In 2021, 905 health data breaches were reported and, according to Protenus's assessment, although a record number of data breaches were reported, the impact of breaches continues to be underreported overall and underrepresented to the public.[8] In 2022, 956 health data breaches were reported in a steady increase year over year, with approximately 60 million patient records affected.[9]

35. PII/PHI is a valuable property right.[10] The value of PII/PHI as a commodity is measurable.[11] "Firms are now able to attain significant market valuations by employing business models predicated on the successful use of personal data within the existing legal and regulatory

---

[6] Protenus, *2021 Breach Barometer*, PROTENUS.COM, https://www.protenus.com/resources/2021-breach-barometer (last accessed Dec. 18, 2024).
[7] Protenus, *2020 Breach Barometer*, PROTENUS.COM, https://www.protenus.com/resources/2020-breach-barometer (last accessed Dec. 18, 2024).
[8] Protenus, *2022 Breach Barometer*, PROTENUS.COM, https://www.protenus.com/hubfs/Breach_Barometer/BreachBarometer_Privacy_2022_Protenus.pdf?utm_campaign=Forbes%2520Articles&utm_source=forbes&utm_medium=article&utm_content=breach%2520barometer (last accessed Dec. 18, 2024).
[9] Protenus, *2023 Breach Barometer*, PROTENUS.COM, https://email.protenus.com/hubfs/Breach_Barometer/2023/BreachBarometer_Privacy_2023_Protenus.pdf (last accessed Dec. 18, 2024).
[10] *See* Marc van Lieshout, *The Value of Personal Data*, 457 International Federation for Information Processing 26 (May 2015) ("The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible…"), https://www.researchgate.net/publication/283668023_The_Value_of_Personal_Data.
[11] *See* Robert Lowes, *Stolen EHR [Electronic Health Record] Charts Sell for $50 Each on Black Market*, MEDSCAPE.COM (April 28, 2014), http://www.medscape.com/viewarticle/824192.

frameworks."[12] American companies are estimated to have spent over $19 billion on acquiring personal data of consumers in 2018.[13] It is so valuable to identity thieves that once PII/PHI has been disclosed, criminals often trade it on the "cyber black-market," or the "dark web," for many years.

36. As a result of its real value and the recent large-scale data breaches, identity thieves and cybercriminals have openly posted credit card numbers, Social Security numbers ("SSNs"), and other sensitive information directly on various internet websites, making the information publicly available. This information from various breaches, including the information exposed in the Data Breach, can be aggregated and become more valuable to thieves and more damaging to victims.

37. PHI is particularly valuable and has been referred to as a "treasure trove for criminals."[14] A cybercriminal who steals a person's PHI can end up with as many as "seven to ten personal identifying characteristics of an individual."[15] A study by Experian found that the "average total cost" of medical identity theft is "about $20,000" per incident, and that a majority of victims of medical identity theft were forced to pay out-of-pocket costs for health care they did not receive in order to restore coverage.[16]

---

[12] OECD, *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD iLIBRARY (April 2, 2013), https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en.

[13] IAB Data Center of Excellence, *U.S. Firms to Spend Nearly $19.2 Billion on Third-Party Audience Data and Data-Use Solutions in 2018, Up 17.5% from 2017*, IAB.COM (Dec. 5, 2018), https://www.iab.com/news/2018-state-of-data-report/.

[14] *See* Andrew Steager, *What Happens to Stolen Healthcare Data*, HEALTHTECH MAGAZINE (Oct. 20, 2019), https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon (quoting Tom Kellermann, Chief Cybersecurity Officer, Carbon Black, stating "Health information is a treasure trove for criminals.").

[15] *Id.*

[16] *See* Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (Mar. 3, 2010), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims.

38. All-inclusive health insurance dossiers containing sensitive health insurance information, names, addresses, telephone numbers, email addresses, SSNs, and bank account information, complete with account and routing numbers, can fetch up to $1,200 to $1,300 each on the black market.[17] According to a report released by the Federal Bureau of Investigation's ("FBI") Cyber Division, criminals can sell healthcare records for 50 times the price of a stolen Social Security or credit card number.[18]

39. Criminals can use stolen PII/PHI to extort a financial payment by "leveraging details specific to a disease or terminal illness."[19] Quoting Carbon Black's Chief Cybersecurity Officer, one recent article explained: "Traditional criminals understand the power of coercion and extortion . . . By having healthcare information—specifically, regarding a sexually transmitted disease or terminal illness—that information can be used to extort or coerce someone to do what you want them to do."[20]

40. Consumers place a high value on the privacy of that data. Researchers shed light on how much consumers value their data privacy—and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[21]

---

[17] SC Staff, *Health Insurance Credentials Fetch High Prices in the Online Black Market*, SC MAGAZINE (July 16, 2013), https://www.scmagazine.com/news/breach/health-insurance-credentials-fetch-high-prices-in-the-online-black-market.

[18] Federal Bureau of Investigation, *Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain* (April 8, 2014), https://www.illuminweb.com/wp-content/uploads/ill-mo-uploads/103/2418/health-systems-cyber-intrusions.pdf.

[19] *What Happens to Stolen Healthcare Data*, *supra* at n.13.

[20] *Id.*

[21] Janice Y. Tsai, et al., *The Effect of Online Privacy Information on Purchasing Behavior, An Experimental Study*, 22(2) INFORMATION SYSTEMS RESEARCH 254 (June 2011) https://www.jstor.org/stable/23015560?seq=1.

41. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' PII/PHI has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

***Theft of PII/PHI Has Grave and Lasting Consequences for Victims***

42. Theft of PII/PHI is serious. The FTC warns consumers that identity thieves use PII/PHI to exhaust financial accounts, receive medical treatment, start new utility accounts, and incur charges and credit in a person's name.[22]

43. Identity thieves use personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[23] According to Experian, one of the largest credit reporting companies in the world, "[t]he research shows that personal information is valuable to identity thieves, and if they can get access to it, they will use it" to among other things: open a new credit card or loan; change a billing address so the victim no longer receives bills; open new utility accounts; obtain a mobile phone; open a bank account and write bad checks; use a debit card number to withdraw funds; obtain a new driver's license or ID; use the victim's information in the event of arrest or court action.[24]

---

[22] *See* Federal Trade Commission, *What to Know About Identity Theft*, FEDERAL TRADE COMMISSION CONSUMER INFORMATION, https://www.consumer.ftc.gov/articles/what-know-about-identity-theft (last accessed Mar. 12, 2024).

[23] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 12 C.F.R. § 1022.3(h). The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number". 12 C.F.R. § 1022.3(g).

[24] *See* Susan Henson, *What Can Identity Thieves Do with Your Personal Information and How Can You Protect Yourself?*, EXPERIAN (Sept. 1, 2017), https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/.

44. Identity theft is not an easy problem to solve. In a survey, the Identity Theft Resource Center found that most victims of identity crimes need more than a month to resolve issues stemming from identity theft and some need over a year.[25]

45. Theft of PII is even more serious when it includes theft of PHI. Data breaches involving medical information "typically leave[] a trail of falsified information in medical records that can plague victims' medical and financial lives for years."[26] It "is also more difficult to detect, taking almost twice as long as normal identity theft."[27] In warning consumers on the dangers of medical identity theft, the FTC states that an identity thief may use PII/PHI "to see a doctor, get prescription drugs, buy medical devices, submit claims with your insurance provider, or get other medical care."[28] The FTC also warns, "If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."[29]

46. A report published by the World Privacy Forum and presented at the U.S. FTC Workshop on Informational Injury describes what medical identity theft victims may experience:

- Changes to their healthcare records, most often the addition of falsified information, through improper billing activity or activity by imposters. These changes can affect the healthcare a person receives if the errors are not caught and corrected.
- Significant bills for medical goods and services not sought nor received.
- Issues with insurance, co-pays, and insurance caps.

---

[25] Identity Theft Resource Center, *2021 Consumer Aftermath Report*, IDENTITY THEFT RESOURCE CENTER (2021), https://www.idtheftcenter.org/identity-theft-aftermath-study/ (last accessed Dec. 18, 2024).
[26] Pam Dixon and John Emerson, *The Geography of Medical Identity Theft*, FTC.GOV (Dec. 12, 2017), https://www.worldprivacyforum.org/2017/12/new-report-the-geography-of-medical-identity-theft/.
[27] *See Health Care Systems and Medical Devices at Risk…*, *supra* at n.15.
[28] *See* Federal Trade Commission, *What to Know About Medical Identity Theft*, Federal Trade Commission Consumer Information, https://www.consumer.ftc.gov/articles/what-know-about-medical-identity-theft (last accessed Dec. 18, 2024).
[29] *Id*.

- Long-term credit problems based on problems with debt collectors reporting debt due to identity theft.

- Serious life consequences resulting from the crime; for example, victims have been falsely accused of being drug users based on falsified entries to their medical files; victims have had their children removed from them due to medical activities of the imposter; victims have been denied jobs due to incorrect information placed in their health files due to the crime.

- As a result of improper and/or fraudulent medical debt reporting, victims may not qualify for mortgage or other loans and may experience other financial impacts.

- Phantom medical debt collection based on medical billing or other identity information.

- Sales of medical debt arising from identity theft can perpetuate a victim's debt collection and credit problems, through no fault of their own.[30]

47. There may also be a time lag between when sensitive personal information is stolen, when it is used, and when a person discovers it has been used. For example, on average, it takes approximately three months for consumers to discover their identity has been stolen and used and it takes some individuals up to three years to learn that information.[31]

48. It is within this context that Plaintiff and all other Class members must now live with the knowledge that their PII/PHI is forever in cyberspace and was taken by people willing to use the information for any number of improper purposes and scams, including making the information available for sale on the black-market.

49. This stolen PII is then routinely traded on dark web black markets as a simple commodity, with online banking login information costing an average of $100, full credit card

[30] *See The Geography of Medical Identity Theft*, *supra* at 25.
[31] John W. Coffey, *Difficulties in Determining Data Breach Impacts*, 17 Journal of Systemics, Cybernetics and Informatics 9 (2019), http://www.iiisci.org/journal/pdv/sci/pdfs/IP069LL19.pdf.

details and associated details costing between $10 and $100, and comprehensive data packages enabling complete identity theft selling for $1,000.[32]

50. Further, as data breaches become ever more prevalent and as technology advances, computer programs can scan the internet to create a mosaic of information that could be used to link compromised information to a specific individual, called the "mosaic effect." Through this process, names, dates of birth, and contact information, hackers and identity thieves can access users' other accounts by, for example, bypassing security questions.

51. Thus, cybercriminals are able to use Plaintiff's and Class Members' Private Information to access email accounts and financial accounts and commit frauds against Plaintiff and Class Members, even when a specific category of information is not compromised in a given breach.

52. A particularly troubling development of cyber-crime are "Fullz" packages. A "Fullz" package is a dosser of information that cybercriminals and other unauthorized parties can assemble by cross-referencing the Private Information compromised in one data breach to publicly available data or data compromised in other data breaches. Automated programs can and are routinely used to create these fullz dossiers, and they typically represent an alarmingly accurate and complete profile of a given individual.

53. Thus, through "Fullz" packages, stolen Private Information from this Data Breach can be easily linked to Plaintiff's and the proposed Class's phone numbers, email addresses, and other sources and identifiers. Thus, even if certain information such as emails, phone numbers, or credit card or financial account were not compromised in this Data Breach, criminals can easily

[32] Ryan Smith, *Revealed-how much is personal information worth on the dark web?*, Insurance News (May 1, 2023), available at https://www.insurancebusinessmag.com/us/news/breaking-news/revealed--how-much-is-personal-information-worth-on-the-dark-web-444453.aspx.

create a Fullz package to sell for profit.

54. Upon information and belief, Plaintiff's and Class members' data have already been accessed and uploaded to the dark web for sale and for identity theft and abuse. A reasonable trier of fact will find that Plaintiff and other Class Members' stolen Private Information is being misused, will continue to be misused, and that such misuse is fairly traceable to the Data Breach.

***Damages Sustained by Plaintiff and the Other Class Members***

55. Plaintiff and all other Class members have suffered injury and damages, including, but not limited to: (i) a substantial increase in the likelihood of identity theft; (ii) the compromise, publication, and theft of their PII/PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with effort attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII/PHI which remains in AJH's possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII/PHI compromised as a result of the Data Breach; and (vii) of overpayment for the services that were received without adequate data security.

***Defendant had a Duty to Protect the Private Information***

56. Defendant has an obligation to protect the Private Information belonging to Plaintiff and Class members. First, this obligation was mandated by government regulations and state laws, including HIPAA and FTC rules and regulations. Second, this obligation arose from industry standards regarding the handling of sensitive PII and medical records. Plaintiff and Class members provided, and Defendant obtained, their information on the understanding that it would be protected and safeguarded from unauthorized access or disclosure.

**HIPAA Requirements and Violation**

57. HIPAA requires, *inter alia*, that Covered Entities and Business Associates implement and maintain policies, procedures, systems and safeguards that ensure the confidentiality and integrity of consumer and patient PII and PHI, protect against any reasonably anticipated threats or hazards to the security or integrity of consumer and patient PII and PHI, regularly review access to data bases containing protected information, and implement procedures and systems to detect, contain, and correct any unauthorized access to protected information. *See* 45 CFR § 164.302, *et seq.*

58. HIPAA, as applied through federal regulations, also requires private information to be stored in a manner that renders it, "unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology. . . ." 45 CFR § 164.402.

59. The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, requires entities to provide notice of a data breach to each affected individual "without unreasonable delay and ***in no case later than 60 days following discovery of the breach***" (emphasis added).

60. Defendant failed to implement and/or maintain procedures, systems, and safeguards to protect the Private Information belonging to Plaintiff and Class members from unauthorized access and disclosure.

61. Upon information and belief, Defendant's security failures include, but are not limited to:

a. Failing to maintain an adequate data security system to prevent data loss;

b. Failing to mitigate the risks of a data breach and loss of data;

c. Failing to ensure the confidentiality and integrity of electronic protected health information Defendant creates, receives, maintains, and transmits in violation of 45 CFR 164.306(a)(1);

d. Failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights in violation of 45 CFR 164.312(a)(1);

e. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 CFR 164.308(a)(1);

f. Failing to identify and respond to suspected or known security incidents;

g. Failing to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity, in violation of 45 CFR 164.308(a)(6)(ii);

h. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic protected health information, in violation of 45 CFR 164.306(a)(2);

i. Failing to protect against any reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 CFR 164.306(a)(3);

j. Failing to ensure compliance with HIPAA security standard rules by Defendant's workforce, in violation of 45 CFR 164.306(a)(94); and

k. Impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons, in violation of 45 CFR 164.502, *et seq.*

62. Upon information and belief, Defendant also failed to store the information it collected in a manner that rendered it, "unusable, unreadable, or indecipherable to unauthorized persons," in violation of 45 CFR § 164.402.

63. Defendant also violated the HIPAA Breach Notification Rule since it did not inform Plaintiff and Class members about the breach until over three months after it first discovered the breach.

**FTC Act Requirements and Violations**

64. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision making. Indeed, the FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

65. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.[33] The guidelines note businesses should protect the personal information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems.[34] The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[35] Defendant clearly failed to do any of the foregoing, as evidenced by the length of the Data Breach, the fact that the Breach went undetected, and the amount of data exfiltrated.

[33] *Protecting Personal Information: A Guide for Business*, Federal Trade Comm'n (October 2016), available at https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business (last accessed Dec. 18, 2024).
[34] *Id.*
[35] *Id.*

66. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction, limit access to sensitive data, require complex passwords to be used on networks, use industry-tested methods for security, monitor the network for suspicious activity, and verify that third-party service providers have implemented reasonable security measures.

67. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data by treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by the FTC Act. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

68. Additionally, the FTC Health Breach Notification Rule obligates companies that suffered a data breach to provide notice to every individual affected by the data breach, as well as notifying the media and the FTC. *See* 16 CFR 318.1, *et seq.*

69. As evidenced by the Data Breach, Defendant failed to properly implement basic data security practices. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiff's and Class members' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act.

70. Defendant was fully aware of its obligation to protect the Private Information of its current and former patients, including Plaintiff and Class members. Defendant is a sophisticated and technologically savvy business that relies extensively on technology systems and networks to maintain its practice, including storing its patients' PII, protected health information, and medical information in order to operate its business.

71. Defendant had and continues to have a duty to exercise reasonable care in collecting, storing, and protecting Private Information from the foreseeable risk of a data breach. The duty arises out of the special relationship that exists between Defendant and Plaintiff and Class members. Defendant alone had the exclusive ability to implement adequate security measures to its cyber security network to secure and protect Plaintiff's and Class members' Private Information.

**Industry Standards and Noncompliance**

72. As noted above, experts studying cybersecurity routinely identify businesses as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

73. Some industry best practices that should be implemented by businesses dealing with sensitive Private Information, like Defendant, include but are not limited to: educating all employees, strong password requirements, multilayer security including firewalls, anti-virus and anti-malware software, encryption, multi-factor authentication, backing up data, and limiting which employees can access sensitive data. As evidenced by the Data Breach, Defendant failed to follow some or all of these industry best practices.

74. Other best cybersecurity practices that are standard in the industry include: installing appropriate malware detection software; monitoring and limiting network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protecting physical security systems; and training staff regarding these points. As evidenced by the Data Breach, Defendant failed to follow these cybersecurity best practices.

75. Defendant should have also followed the minimum standards of any one of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

76. Defendant failed to comply with these accepted standards, thereby permitting the Data Breach to occur.

## PLAINTIFF'S EXPERIENCES

77. Plaintiff Preston Leonard is a former patient of Anna Jaques Hospital.

78. Plaintiff Preston Leonard received AJH's data breach notice dated December 5, 2024. The notice informed Plaintiff Preston Leonard that his Private Information was improperly accessed and obtained by third parties and that this information included his name, date of birth, medical information, health insurance information, patient name, and patient address.

79. As a result of the Data Breach, Plaintiff Preston Leonard has made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching the Data Breach and reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud.

80. Plaintiff Preston Leonard receives notifications regarding unknown parties attempting to login and access various online accounts as well as credit alerts from his financial institution. He spends about 20 minutes each week dealing with the Data Breach, valuable time he otherwise would have spent on other activities, including, but not limited to, work and recreation.

81. Plaintiff Preston Leonard suffered actual injury from having his Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of his Private Information, a form of property that Defendant obtained from him; (b) violation of his privacy rights; and (c) present, imminent and impending injury arising from the increased risk of identity theft and fraud.

82. Plaintiff Leonard is especially concerned about the likelihood that, as a consequence of AJH's Data Breach, his previously confidential medical data may be in the hands of computer hackers, and/or for sale on the dark web.

83. As a result of the Data Breach, Preston Leonard anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. And, as a result of the Data Breach, he is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

## CLASS ALLEGATIONS

84. This action is brought and may be properly maintained as a class action pursuant to Fed. R. Civ. P. 23.

85. Plaintiff brings this action individually and on behalf of all members of the following Class of similarly situated persons:

> All persons in the United States whose Private Information was accessed in the Data Breach and including those who were sent notice by AJH.

86. Excluded from the Class are: (1) the Judges presiding over the action and members of their families; (2) Anna Jaques Hospital, and its affiliates, parents, subsidiaries, officers, agents, and directors; (3) Beth Israel Lahey Health, Inc., and its affiliates, parents, subsidiaries, officers, agents, and directors; (4) natural persons who properly submit a timely request for exclusion from the Class; and (5) the successors or assigns of any such excluded natural person.

87. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of their claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

88. The members in the Class are so numerous that joinder of all Class members in a single proceeding would be impracticable. AJH has not yet publicly announced the number of individuals whose Private Information was exposed in the Data Breach, but upon information and belief, the number is in the tens of thousands. The members of the Class will be identifiable through information and records in AJH's possession, custody, and control.

89. Common questions of law and fact exist as to all Class members and predominate over any potential questions affecting only individual Class members. Such common questions of law or fact include, *inter alia*:

a. Whether AJH had a duty to implement and maintain reasonable security procedures and practices to protect and secure Plaintiff's and Class Members' PII/PHI from unauthorized access and disclosure;

b. Whether AJH failed to exercise reasonable care to secure and safeguard Plaintiff's and Class Members' PII/PHI;

c. Whether an express and/or implied contract existed between Class members and AJH providing that AJH would implement and maintain reasonable security measures to protect and secure Class members' PII/PHI from unauthorized access and disclosure;

d. Whether AJH breached its duties to protect Plaintiff's and Class members' PII/PHI; and

e. Whether Plaintiff and all other members of the Class are entitled to damages and the measure of such damages and relief.

90. AJH engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff on behalf of themselves and all other Class members. Individual questions, if any, pale in comparison, in both quantity and quality, to the numerous common questions that dominate this action.

91. Plaintiff's claims are typical of the claims of the Class. Plaintiff, like all proposed members of the Class, had PII/PHI compromised in the Data Breach. Plaintiff and Class members were injured by the same wrongful acts, practices, and omissions committed by AJH, as described herein. Plaintiff's claims therefore arise from the same practices or course of conduct that give rise to the claims of all Class members.

92. Plaintiff will fairly and adequately protect the interests of the Class members. Plaintiff is an adequate representative of the Class in that Plaintiff has no interests adverse to, or that conflict with, the Class she seeks to represent. Plaintiff has retained counsel with substantial experience and success in the prosecution of complex consumer protection class actions of this nature.

93. A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages and other financial detriment suffered by Plaintiff and all other Class members are relatively small compared to the burden and expense that would be required to individually litigate their claims against AJH, so it would be impracticable for Class members to individually seek redress from AJH's wrongful conduct. Even if Class members could afford individual litigation, the court system could not. Individualized litigation creates a potential

for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

## CAUSES OF ACTION

### COUNT I
### NEGLIGENCE

94. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

95. AJH owed a duty to Plaintiff and all other Class members to exercise reasonable care in safeguarding and protecting their PII/PHI in its possession, custody, or control.

96. AJH knew the risks of collecting and storing Plaintiff's and all other Class members' PII/PHI and the importance of maintaining secure systems. AJH knew of the many data breaches that targeted healthcare providers in recent years.

97. Given the nature of AJH's business, the sensitivity and value of the PII/PHI it maintains, and the resources at its disposal, AJH should have identified the vulnerabilities to their systems and prevented the Data Breach from occurring.

98. AJH breached these duties by failing to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII/PHI by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect PII/PHI entrusted to it—including Plaintiff's and Class members' PII/PHI.

99. It was reasonably foreseeable to AJH that its failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII/PHI by failing to design, adopt,

implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems would result in the unauthorized release, disclosure, and dissemination of Plaintiff's and Class members' PII/PHI to unauthorized individuals.

100. But for AJH's negligent conduct or breach of the above-described duties owed to Plaintiff and Class members, their PII/PHI would not have been compromised.

101. AJH's violations of HIPAA Privacy and Security Rules and Section 5 of the FTCA constitute negligence per se.

102. Plaintiff and Class members are within the class of persons that HIPAA Privacy and Security Rules and Section 5 of the FTCA were intended to protect.

103. The harm occurring as a result of the Data Breach is the type of harm HIPAA Privacy and Security Rules and Section 5 of the FTCA were intended to guard against.

104. It was reasonably foreseeable to AJH that its failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII/PHI by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems, would result in the release, disclosure, and dissemination of Plaintiff's and Class members' PII/PHI to unauthorized individuals.

105. The injury and harm that Plaintiff and the other Class members suffered was the direct and proximate result of AJH's violations of HIPAA Privacy and Security Rules and Section 5 of the FTCA.

106. As a result of AJH's above-described wrongful actions, inaction, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiff and all other Class

members have suffered, and will continue to suffer, economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantially increased risk of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII/PHI; (iii) breach of the confidentiality of their PII/PHI; (iv) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII/PHI compromised as a result of the Data Breach; and (vii) of overpayment for the services that were received without adequate data security.

**COUNT II**
**BREACH OF FIDUCIARY DUTY**

107. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

108. As a condition of obtaining services from AJH, Plaintiff and Class members gave Defendant their PII/PHI in confidence, believing that Defendant would protect that information.

109. Plaintiff and Class members would not have provided Defendant with this information had they known it would not be adequately protected. AJH's acceptance, use, and storage of Plaintiff's and Class members' Private Information created a fiduciary relationship between Defendant and Plaintiff and Class members. In light of this relationship, Defendant must act primarily for the benefit of their patients, which includes safeguarding and protecting Plaintiff's and Class members' Private Information.

110. Defendant has a fiduciary duty to act for the benefit of Plaintiff and Class members upon matters within the scope of their relationship. AJH breached that duty by,

among other things, failing to properly protect the integrity of the system containing Plaintiff's and Class members' Private Information, failing to comply with the data security guidelines set forth by HIPAA, and otherwise failing to safeguard Plaintiff's and Class members' Private Information that it collected, utilized, and maintained.

111. As a direct and proximate result of AJH's breach of its fiduciary duties, Plaintiff and Class members have suffered and will suffer injury, including, but not limited to: (i) a substantially increased and imminent risk of identity theft; (ii) the compromise, publication, and theft of their PII/PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with efforts attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII/PHI which remains in AJH's possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII/PHI compromised as a result of the Data Breach; and (vii) overpayment for the services that were received without adequate data security.

112. AJH violated HIPAA Privacy and Security Rules and Section 5 of the FTCA by failing to use reasonable measures to protect Plaintiff's and all other Class members' PII/PHI and not complying with applicable industry standards. AJH's conduct was particularly unreasonable given the nature and amount of PII/PHI it obtains and stores, and the foreseeable consequences of a data breach involving PII/PHI including, specifically, the substantial damages that would result to Plaintiff and the other Class members.

## COUNT III
## BREACH OF IMPLIED CONTRACT

113. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

114. In connection with receiving medical services, Plaintiff and all other Class members entered into implied contracts with AJH and/or BILH.

115. Pursuant to these implied contracts, Plaintiff and Class members paid money to AJH, whether directly or through their insurers, and provided AJH with their PII/PHI. In exchange, AJH agreed to, among other things, and Plaintiff understood that AJH would: (1) provide medical services to Plaintiff and Class member; (2) take reasonable measures to protect the security and confidentiality of Plaintiff's and Class members' PII/PHI; and (3) protect Plaintiff's and Class members PII/PHI in compliance with federal and state laws and regulations and industry standards.

116. The protection of PII/PHI was a material term of the implied contracts between Plaintiff and Class members, on the one hand, and AJH, on the other hand. Indeed, as set forth *supra*, AJH recognized the importance of data security and the privacy of its patients' PII/PHI in its Privacy Notice. Had Plaintiff and Class members known that AJH and/or BILH would not adequately protect its patients' and former patients' PII/PHI, they would not have received medical services from AJH.

117. Plaintiff and Class members performed their obligations under the implied contract when they provided AJH with their PII/PHI and paid—directly or through their insurers—for health care services from AJH.

118. AJH breached its obligations under its implied contracts with Plaintiff and Class members in failing to implement and maintain reasonable security measures to protect and secure their PII/PHI and in failing to implement and maintain security protocols and procedures to protect Plaintiff's and Class members' PII/PHI in a manner that complies with applicable laws, regulations, and industry standards.

119. AJH's breach of its obligations of its implied contracts with Plaintiff and Class members directly resulted in the Data Breach and the injuries that Plaintiff and all other Class members have suffered from the Data Breach.

120. Plaintiff and all other Class members were damaged by AJH's breach of implied contracts because: (i) they paid—directly or through their insurers—for data security protection they did not receive; (ii) they face a substantially increased risk of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (iii) their PII/PHI was improperly disclosed to unauthorized individuals; (iv) the confidentiality of their PII/PHI has been breached; (v) they were deprived of the value of their PII/PHI, for which there is a well-established national and international market; (vi) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face; and (vii) of overpayment for the services that were received without adequate data security.

## COUNT IV
## UNJUST ENRICHMENT

121. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

122. This claim is pleaded in the alternative to the breach of implied contract claim.

123. Plaintiff and Class members conferred a monetary benefit upon AJH in the form of monies paid for healthcare services or other services.

124. AJH accepted or had knowledge of the benefits conferred upon it by Plaintiff and Class Members. AJH also benefitted from the receipt of Plaintiff's and Class members' PII/PHI, as this was used to facilitate payment.

125. As a result of AJH's conduct, Plaintiff and Class members suffered actual damages in an amount equal to the difference in value between their payments made with reasonable data privacy and security practices and procedures that Plaintiff and Class members paid for, and those payments without reasonable data privacy and security practices and procedures that they received.

126. AJH should not be permitted to retain the money belonging to Plaintiff and Class members because AJH failed to adequately implement the data privacy and security procedures for itself that Plaintiff and Class members paid for and that were otherwise mandated by federal, state, and local laws and industry standards.

127. AJH should be compelled to provide for the benefit of Plaintiff and Class members all unlawful proceeds received by it as a result of the conduct and Data Breach alleged herein.

## PRAYER FOR RELIEF

Plaintiff, individually and on behalf of all other members of the Class, respectfully requests that the Court enter judgment in Plaintiff's favor and against AJH as follows:

A. Certifying the Class as requested herein, designating Plaintiff as class representative, and appointing Plaintiff's counsel as Class Counsel;

B. Awarding Plaintiff and the Class appropriate monetary relief, including actual damages, statutory damages, punitive damages, restitution, and disgorgement;

C. Awarding Plaintiff and the Class equitable, injunctive, and declaratory relief, as may be appropriate. Plaintiff, individually and on behalf of the Class, seeks appropriate injunctive relief designed to prevent AJH from experiencing another data breach by adopting and implementing best data security practices to safeguard PII/PHI and to provide or extend credit monitoring services and similar services to protect against all types of identity theft and medical identity theft;

D. Awarding Plaintiff and the Class pre-judgment and post-judgment interest to the maximum extent allowable;

E. Awarding Plaintiff and the Class reasonable attorneys' fees, costs, and expenses, as allowable; and

F. Awarding Plaintiff and the Class such other favorable relief as allowable under law.

**JURY TRIAL DEMANDED**

Plaintiff demands a trial by jury of all claims in this Class Action Complaint so triable.

December 23, 2024

*/s/Sean K. Collins*
Sean K. Collins (BBO 687158)
**LAW OFFICES OF SEAN K. COLLINS**
184 High Street, Suite 503
Boston, MA 02110
Telephone: 855-693-9256
Fax: 617-227-2843
skc@seankcollinslaw.com

Gary E. Mason*
Lisa A. White*
**MASON LLP**
5335 Wisconsin Avenue, NW, Suite 640
Washington, DC 20015
Tel: (202) 429-2290
Email: gmason@masonllp.com
Email: lwhite@masonllp.com

*Counsel for Plaintiff*

**Pro hac vice* applications to follow